



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/698,197	10/31/2003	Pradipta Kumar Banerjee	JP920030162US1	9974
36903 7590 10/17/2008 IBM ENDICOTT (ANTHONY ENGLAND) LAW OFFICE OF ANTHONY ENGLAND PO Box 5307 AUSTIN, TX 78763-5307				
EXAMINER OSMAN, RAMY M				
ART UNIT 2457		PAPER NUMBER		
MAIL DATE 10/17/2008		DELIVERY MODE PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/698,197

**Applicant(s)**

BANERJEE ET AL.

**Examiner**

RAMY M. OSMAN

**Art Unit**

2457

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 04 August 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-4, 7, 9-11, 13-16, 19-23, 25-28, 31, 33, 34 and 36-44 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-4, 7, 9-11, 13-16, 19-23, 25-28, 31, 33, 34 and 36-44 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Final Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Status of Claims***

1. This action is responsive to amendment filed on August 4, 2008, where applicant amended claims 1,2,7,13,14,19,20,25,26,31 and added new claims 36-44. Claims 1-4,7,9-11,13-16,19-23,25-28,31,33,34 and 36-44 are pending.

### ***Response to Arguments***

2. Applicant's arguments, filed 8/4/2008, with respect to the rejection(s) of claim(s) 1-4,7,9-11,13-16,19-23,25-28,31 and 33-34 have been fully considered and are persuasive. The previous rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of **Yadav (US Patent No 7174566)**, as outlined below. Applicants arguments are therefore moot in view of the new grounds of rejection.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 1-4,7,9-11,13-16,19-23,25-28,31,33,34 and 36-44 rejected under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061).**

5. In reference to claim 1, Yadav teaches a method of detecting an intrusion in a communications network, the method comprising the steps of:

a) accessing, by a network intrusion detection process of a target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system, wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the application from the transport layer (column 5 lines 14-32);

b) scanning for the application by the network intrusion detection process only the data packets accessed .by the network intrusion detection process in a), wherein the data packets are directed to the application from a remote host via the communications network, and wherein the scanning is after the data .packets have been processed by the e-transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ (column 6 lines 17-37);

c) determining if said scanned data packets are malicious (column 6 lines 45-47); and

d) taking at least one action to prevent the application from processing data packets from the remote host to the application responsive to c) determining that any of the scanned data packets are malicious (column 6 lines 25-67 & 54-67).

Although Yadav teaches application level components to which particular communications are sent to and from (column 5 lines 14-30), Yadav fails to explicitly teach application receive queue (ARQ) functioning intermediate a transport layer and an application layer to receive data packets for the application. However, Holland teaches host-based

monitoring of a network protocol stack (column 5 lines 23-45). Holland discloses monitoring via queues intermediate application and transport layers for providing and scanning data for intrusion detection, and further discloses scanning between the TCP layer (Figure 4 and column 6 lines 35-61). It would have been obvious for one of ordinary skill in the art to modify Yadav wherein at least one application receive queue (ARQ) functions intermediate said transport layer and an application layer of the first computer system provides the queue for data, as per the teachings of Holland for the purpose of implementing intrusion detection within the different levels of a protocol stack.

6. In reference to claim 2, Yadav teaches the method according to claim 1. Although Yadav teaches tracking abnormally behaving applications (column 5 lines 47-52), Yadav fails to explicitly teach wherein said at least one action includes terminating the application. However, it is common knowledge that if an application is behaving abnormally, and that it is possible due to an intrusion, then that application should be terminated in order to prevent any harmful effects that may result from the intrusion. It would have been obvious for one of ordinary skill in the art to modify Yadav wherein said at least one action includes terminating the application in order to prevent any harmful effects that may result from the intrusion.

7. In reference to claim 3, Yadav teaches the method according to claims, further comprising the step of transmitting to said application layer any data packets determined not to be malicious (column 6 lines 25-37).

8. In reference to claim 4, Yadav teaches the method according to claim 1, wherein said scanning and determining steps are implemented using a scan module (column 6 lines 45-47).

9. In reference to claim 7, Yadav teaches the method according to claim 6, further comprising the step of obtaining data from said at least one ARQ (Holland, Figure 4 and column 6 lines 35-61, see rationale for claim 1 above).
10. In reference to claim 9, Yadav teaches the method according to claim 1, further comprising the step of dispatching said data packets to one or more handlers for scanning, if said protocol is monitored (column 6 lines 25-67).
11. In reference to claim 10, Yadav teaches the method according to claim 1, wherein said scanning and determining steps are implemented using a scan daemon (column 6 lines 45-48).
12. In reference to claim 11, Yadav teaches the method according to claim 1, further comprising the step of the target computer system generating fake network accessible services (column 6 lines 54-67).
13. In reference to claim 36, Yadav teaches the method according to claim 1, wherein said at least one action includes modifying firewall rules to prevent reception of data packets from the host computer system (column 7 lines 4-18).
14. In reference to claim 37, Yadav teaches the method according to claim 1, wherein the directing of the data packets to the application from the remote host is via a connection with the remote host on the communications network, and wherein said at least one action includes intimating the transport layer to tear down the remote host connection (column 6 lines 25-31).
15. In reference to claim 38, Yadav teaches the method according to claim 37, wherein after intimating the transport layer to tear down the remote host connection, the target computer services requests on connections other than that remote host connection (column 6 lines 25-31).

16. In reference to claims 13-16,19-23,39-41, these claims are system claims that correspond to the method claims of claims 1-4,7,9-11,36-38. Therefore, claims 13-16,19-23,39-41 are rejected based upon the same rationale as given for claims 1-4,7,9-11,36-38 above.

17. In reference to claims 25-28,31,33,34,42-44, these claims are product claims that correspond to the method claims of claims 1-4,7,9-11,36-38. Therefore, claims 25-28,31,33,34,42-44 are rejected based upon the same rationale as given for claims 1-4,7,9-11,36-38 above.

### *Conclusion*

18. The above rejections are based upon the broadest reasonable interpretation of the claims. Applicant is advised that the specified citations of the relied upon prior art, in the above rejections, are only representative of the teachings of the prior art, and that any other supportive sections within the entirety of the reference (including any figures, incorporation by references, claims and/or priority documents) is implied as being applied to teach the scope of the claims.

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See attached Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RAMY M. OSMAN whose telephone number is (571)272-4008. The examiner can normally be reached on M-F 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (571) 272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ramy M Osman/  
Examiner, Art Unit 2457

October 14, 2008